REMARKS

This Amendment Under 37 C.F.R. §1.116, is in response to the final Office Action mailed May 24, 2007. A Request for Continued Examination (RCE) is filed herewith.

At the outset, the undersigned wishes to thank Exr. Agwumezie for his time, consideration and expert guidance during the recent telephone interview of October 2, 2007. As discussed during the telephone interview, claim 1 and its dependent claims have been canceled, without prejudice to their respective subject matter.

Independent claim 9 has been amended to clearly and positively recite specific and proper method steps that are carried out to validate the authority information within the received certificate, as Exr. Agwumezie counseled the undersigned during the interview.

As amended, independent claim 9 recites:

> **accessing a store of authority information that is coupled to the network and that is independent of the received certificate;**
>
> **retrieving, from the accessed store of authority information, stored authority information that is associated with the user;**
>
> **comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate;**
>
> **validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate, and**
>
> **executing of the payment request only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate is successfully validated.**

Independent claims 15 and 29 have been similarly amended.

Therefore, each claim recites that the authority of the user defined in the second code portion of the certificate is verifiable independently of the digital certificate. This is done, according to the claims, by accessing a store of authority information that is independent of the digital certificate; retrieving, from the accessed store of authority information, stored authority

information that is associated with the user; comparing the retrieved authority information with the authority information included within the received certificate to determine whether the retrieved authority information matches the authority information included within the received certificate, and validating the authority information within the received certificate only if the retrieved authority information matches the authority information included within the received certificate. Thereafter, only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate are successfully validated is the payment request executed, as claimed. As the Examiner will note the amended claims recite a series of explicit steps, and are not narrative in nature, to specifically address the Examiner's concerns voiced during the telephone and also memorialized in the Advisory Action.

It is respectfully submitted that the claims recite that the authority defined within the certificate is verifiable (or may be validated) by accessing a store of information that is independent of the digital certificate. Moreover, it is acknowledged that the primary combination to Brown et al. and Hwangbo do not teach or suggest such subject matter, which necessitated the addition of Sudia et al. to the applied combination.

The Office points to paragraphs [0132], [0171], and [0252] for a teaching of verifying the authority of the user defined within the second code portion of the certificate by the server computer independently of the digital certificate by accessing, over the network, a store of authority information that is independent of the digital certificate and by matching the authority of the user defined within the second code portion of the certificate to corresponding authority information of the user retrieved from the accessed independent store of authority information, as claimed.

Sudia et al. rely upon a plurality of trusted devices (such as signing devices 1, 2, 3, 4 and 5 of Fig. 1), each associated with an authorizing agent (1a, 2a, 3a, 4a and 5a of Fig. 1), all coupled via a WAN/LAN 21. In Sudia et al., each of the trusted devices, as instructed by its associated authorizing agent(s), affixes a partial digital signature to a document (for example) to be digitally signed in response to the authorization of a quorum (predetermined number) of authorizing agents, as described in paragraph [0085]. Therefore, Sudia et al. teach that there is a plurality of trusted devices, and each trusted device is configured to affix only a partial signature, and only when requested to by a predetermined number of authorizing agents. Thereafter, the trusted device returns the fully signed result to the requester (if all other required trusted devices have already signed) or routes the partially signed result to the next trusted device in the protocol, as described in paragraph 4, lines 8-12:

> than they can be processed. The message server presents messages to the signing device for signing, receives the signed (or partially signed) result, and either (a) returns the partially signed result to the requester, or (b) routes the result to the next device in the protocol. In order to receive and

The "authorizing agents" in Sudia et al. issue signing instructions to the trusted device to which he or she is associated. See paragraph [0054]. Each trusted device has a signature, as does each authorizing agent, and they are used for different purposes, as detailed in Sudia et al. at paragraph 55, lines 8-12:

> erated for and certified as belonging to the specified user. In this manner, the system can continue to use the device's signature to verify the trust level of the device on any given transaction, while using the user's signature to attest to the user's identity and consent to the transaction. This allows the

The authority of an authorized agent, in Sudia et al., is the authority of the authorizing agent to request that his or her associated trusted device digitally sign the document or message, not to request that a server computer carry out a requested action, as claimed herein. The list of such authorizing agents is maintained in an internal table (see Fig. 7)

as discussed in Sudia et al. at paragraph [0132] (one of the paragraphs referenced in the Office Action), of which lines 7-11 are reproduced below:

> verification key for each authorizing agent. In the registration process, each signing device will also update an internally-stored table of particular authorizing agents who will be empowered to instruct the signing device to apply its partial signature. During routine operation, a signing device

Therefore, when requested to partially digitally sign a document or message, the trusted devices of Sudia et al. will consult their internal tables 26 to insure that the requestor is an authorizing agent and only thereafter will the trusted device partially sign the requested document or message.

In Claim 1, the digital certificate is issued to the user of the client computer. In contrast, Sudia et al. teaches a method of digitally signing a message or a document by processing a plurality of partial digital signatures by a plurality of trusted devices on behalf of a corresponding plurality of authorized agents. Therefore, Sudia et al. teach who may sign a document or message and how such document or message may be digitally signed (i.e., by sequential partial signing), whereas the claimed embodiments define methods, code and a software application for validating the authority (by carrying out positively recited steps) within a certificate and executing a payment requests or a request that a server computer carry out a requested action only if the authority is successfully validated, as claimed.

Specifically, the method detailed in Sudia et al. deals with authentication; that is, insuring that those signing a digital certificate (through the trusted devices) are who they purport to be and are authorized to request that their trusted device sign the document or message. Such information, in the claimed embodiment, would be placed in the first claimed portion:

> **wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field,**

and not in the claimed second portion that is configured to define an authority of the user to request that the server computer carry out a requested action, as claimed.

The internal tables (see, e.g., 23 in Fig. 7) of authorizing agents who are "empowered to instruct the signing device to apply its partial signature", according to Sudia et al., do not include any information as to the authorizing agent's authority, within the meaning of the claims. Indeed, claim 9 recites that the authority in question is the authority of the user to make a payment request, and not the authority of an agent to instruct a signing device to apply a digital signature.

Sudia et al. do not teach or suggest any such authority defined within the internal tables of authorizing agents 23. Moreover, when the internal tables 23 of Sudia et al. are consulted, the certificate is not yet in existence (even partially), as the trusted device is still determining whether the requestor is listed as an authorizing agent so that it may partially sign the document or message.

Moreover, kindly note paragraph [0050] of Sudia et al., which states:

> **[0050] FIG. 2** shows a preferred architecture for a secure data center computer configuration **48**, where each signing device of **FIG. 1** preferably will be found. In addition to a signing device **29**, each data center configuration **48** additionally contains a separate message server **47**. The signing device **39** is dedicated to signing operations and is located in a physically secure location, such as a vault. There is no direct connection between the signing device and the external computer network. As will be discussed more fully below, the signing device **39** will be provided with a key share for multi-step signing **36**, its own device signature key **37**, table **38** identifying its authorizing agents, and a certificate for its public verification key **40**, a public key chosen to match its key share **36** (where the certificate is signed by the full KS_{DSA} via the multi-step method).

In contrast, claim 9 specifically requires steps of:

> **accessing a store of authority information that is coupled to the network and that is independent of the received certificate;**
>
> **retrieving, from the accessed store of authority information, stored authority information that is associated with the user;**

That is, the authority is validated by accessing a store of authority information that is coupled to the network, in direct contrast with Sudia et al., which explicitly state that the signing device has no connection to the external computer network.

This claimed recitation is not taught or suggested by Sudia et al., which specifically state that the internal tables of authorizing agents are maintained as internal tables within the trusted signing devices, and that the trusted signing devices have no direct connection to the external computer network, rendering the functionality and the steps recited in the amended claims impossible for the architecture espoused by Sudia et al.

Therefore, Sudia et al., contrary to the claimed embodiments, do not teach accessing, retrieving, comparing and matching the authority information stored in the store of authority information with the authority information within the received digital certificate, as claimed herein.

It is respectfully submitted that a person of ordinary skill in the art in full possession of the Brown-Hwangbo-Sudia combination would be motivated to partially sign (as taught by Sudia et al.) a document or message with a digital certificate (as taught by Brown). The identity of authorizing users, in such a combination, would be stored within internal tables of a trusted signing device, as taught by Sudia et al. Those internal tables, moreover, would be consulted by the trusted signing device without accessing the network, as explicitly taught by Sudia et al., and without accessing, retrieving, comparing and matching the authority information within the certificate to corresponding authority information stored in the store of information that is

independent of the received certificate and that is accessed over the network, as also claimed herein. Nothing in the applied combination, moreover, teaches or suggests the authority in question is the authority to request a server computer to carry out a requested action, as claimed herein. In Sudia et al., for example, the agents are "authorized" to request that the trusted signing devices digitally sign the document or message in question, but are not "authorized to request that a server carry out a requested action. Moreover, the authority of the "authorizing agents", in Sudia et al. is not verified by accessing, retrieving, comparing and matching in the manner claimed herein.

In short, the Brown et al.-Sudia et al. combination does not teach or suggest to verify the authority of the certificate holder (as opposed to the identity of the agent in the internal tables, as in Sudia et al.) by accessing a store of authority information, over the network, that is independent of the received certificate. Again, Sudia et al. do not remedy the acknowledged shortcomings of the Brown reference, because Sudia et al. do not teach certificates assigned a) to users of a client computer b) that define an authority of the certificate holder to request that the server carry out a requested action c) that is verifiable by accessing and retrieving d) over the network of e) a store of authority information that is f) independent of the certificate. Sudia et al. also do not teach comparing the authority information within the certificate to authority information retrieved from the store of authority information, as claimed herein.

Therefore, it is respectfully submitted to Exr. Agwumezie that the applied combination fails to teach or to suggest the claimed embodiments of the presently amended independent claims. Reconsideration and withdrawal of the rejections of claims 9, 15 and 29 and that of their respective dependent claims are, therefore, respectfully requested.

Applicant believes that this application is now in condition for allowance. If any unresolved issues remain, please contact the undersigned attorney of record at the telephone number indicated below and whatever is necessary to resolve such issues will be done at once.

Respectfully submitted,

Date: October 11, 2007 By: _____

Alan W. Young
Attorney for Applicant
Registration No. 37,970

YOUNG LAW FIRM, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

\\Ylfserver\ylf\CLIENTS\ORCL\5881 (OID-2003-142-01)\5881 AMEND.5.doc